ISSN (ONLINE):2045-8711
ISSN (PRINT):2045-869X

International Journal of Innovative Technology and Creative Engineering

April 2024
Vol- 14 No.- 4
@ IJITCE Publication

UK: Managing Editor
International Journal of Innovative Technology and Creative Engineering
1a park lane,
Cranford
London
TW59WA
UK

USA: Editor
International Journal of Innovative Technology and Creative Engineering
Dr. Arumugam
Department of Chemistry
University of Georgia
GA-30602, USA.

India: Editor
International Journal of Innovative Technology & Creative Engineering
36/4 12th Avenue,
1st cross St,
VaigaiColony
Ashok Nagar
Chennai, India 600083

Email: editor@ijitce.co.uk

www.ijitce.co.uk

IJITCE PUBLICATION

International Journal of Innovative Technology & Creative Engineering

Vol.14 No.04

April 2024



www.ijitce.co.uk

Dear Researcher,

Greetings!

Articles in this issue discusses about study endeavors to recent trends in iris image.

We look forward many more new technologies in the next month.

Thanks,
Editorial Team
IJITCE

Editorial Members

Contents

VIDEO STEGANOGRAPHY: A SECURE WAY TO HIDEDATA IN VIDEO FILES

Rao Somaiya Bhasker
CMR University, Bengaluru, India
Dr. Chitra Ravi
CMR University, Bengaluru, India
Dr .Umadevi R
CMR University, Bengaluru, India

Abstract - With the passing of time, humans are slowly becoming slaves of the digital world. In the current scenario, every other person depends on digital media for their day to day operations. With such a huge volume of transactions happening daily over the internet, it is the need of the hour to provide a secure channel to transfer confidential data. There are many cryptographic algorithms and data hiding techniques available to provide a secure way to transfer data from source to destination over the internet, without any unauthorized user getting access to the data. Steganography is one such method of data hiding. Steganography is a technique of hiding data in some media file like text, image, audio, video etc. without being detected by unauthorized users. Video Steganography is the technique of embedding text data in the frames of video, without much distortion of the cover media. There are many algorithms being introduced through all these years to do video steganography with an aim of minimizing the alteration of cover image. The aim of this paper is to study all such algorithms and compare them all.

Keywords: Cryptography, Steganography, Steganalysis, spatial domain , Discrete wavelet transform, LSB, Early Embedding, Delayed Embedding, DCT

I. Introduction

Today in this digitally advanced world where nothing is assumed to be impossible, Along with the developments in techniques of data security, corresponding advancements are made in the field of hacking as well. So, the need for improving data security methods is increasing day by day. Steganography is one of the techniques for securing confidential information across the internet. The word steganography has its origin in Greek. In the word Steganography, stegnos means something that has to be protected and the word graphic means writing. In other words, it can be explained as a secret communication technique in which only the sender and the recipient know about the existence of the message.

Technical definition of Steganography is —Hiding a secret message by embedding the message into some other media file such as text, audio, video etc.

Steganography has gone through much advancement till date. In ancient days the Greeks used to shave the heads of their slaves and write messages there. When the hair grew back, they would send the slaves to recipients who again shaved the heads to read the secret message. This method was really time consuming and offered limited space for writing the message. In another form, steganography was carried out through wax tablets. In this technique, people used to write messages on wood and cover it with wax. Then these wax tablets were sent to the intended receiver where the wax was peeled off in order to read thatmessage. Null ciphers were later on used as steganography during the First and Second World War by the Germans. Here the useful message was encapsulated in a meaningless message. For example the first alphabet of every word of sent message maybe plucked out to reveal the actual message. Later, invisible inks were also used during the American Revolution by revolutionaries. Paper with messages written using such kind of inks were exposed to fire in order to read that message. Today is the era of digital world, digital steganography is used, where secret message is hidden inside another media file such as text, image, audio, video etc.

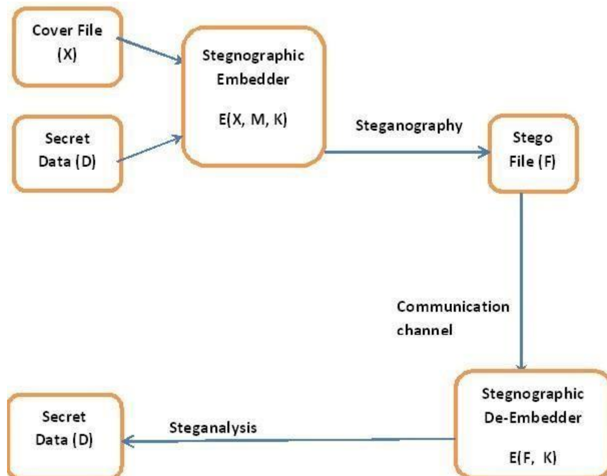


Fig. 1: Basic Steganography model

From Fig. 1 we get the following terms used insteganography

- Cover-File - Unique media file (text, image, audio, video etc.,) that can conceal data.
- Message - Real data that you can mask within cove file. The message may be in the form of standard text or an image or an audio file or video file.
- Stego-File − A stego file is an image with a hidden message.
- Stego-Key - Messages can be embedded in cover files and stego-files with the help of a key, or the messages can be derived from the cover files themselves.

Using above terms we can define this simple formula:

Cover-File +Embedded-Message = Stego-File

II. Problem Statement

Exploring Digital Image and Video Steganography. Understanding and comparing different Steganography techniques.

A wide number of different techniques for image and video steganography has been developed. In video steganography, the cover video is first divided into frames, that are still images extracted from that video. Then any one of the frames is used to embed the secret message in it. After the embedding process is done, the frame is again added into the video in its place. Unlike image steganography, video steganography can be considered better as it is difficult to judge the presence of confidential information in moving frames of video.

While embedding the secret data into cover image there is always a chance of cover image being distorted due to replacing of bits in cover image by data bits. This may lead to identification of hidden data. Because of this the data security over the channel may be compromised. The main aim of this paper is to study and compare all such existing steganography algorithms which will help us to find the limitations of these algorithms and a way to upgrade the algorithm.

III. Steganography Techniques

Steganography technique was first developed in ancient Greece around 400 B.C. Steganography has been in use for 2500 years for various purposes. The major use of these techniques is in the area of military, Banking, intelligence services, personal and Business world [1]. Steganography is the method of sending confidential information to someone without the fear of data being grabbed by the interceptor. Steganography is the technique of disguising the existence of an original message called in the cover media.

Let us now discuss different steganography method being used till date

Primitive Techniques of Steganography:

The history of Steganography takes us back to Greek historian Herodotus in his chronicles known as –Historiesll and date back to around 440 BC. Herodotus recorded two stories of Steganographic techniques during this time in Greece.

a. Around 440 BC in Greece, Kings used to shave the heads of their prisoners and write secret messages on their scalp. When the prisoner‘s hair grew back, the message was hidden beneath the grown hair. The prisoners were then sent to the Kings to whom the messages needed to be delivered. At the destination, kings again shaved back the prisoner‘s head to read the secret message.

b. Another technique also comes from Greece, where soldiers used to send messages by writing text on wax-covered tablets. Soldiers used to remove the wax from the tablet, write the secret message to be delivered on the underlying wood, cover the tablet with wax again to make it appear as a blank tablet and finally send the document without being detected. At the destination the people used invisible inks, which were extracted from the natural substances such as fruit juices and milk. The secret message would be recovered by heating the hidden text, thus revealing its contents.

c. During the 15th and 16th centuries, many writers including Johannes Trithemius who is the author of Steganographia and Gaspari Schotti , author of Steganographica did research and wrote on Steganographic techniques in their books. These authors have mentioned steganographic techniques such as coding techniques for text, invisible inks, and incorporating hidden messages in music in their books. Between 1883 and 1907, further development was done by publications of Auguste Kerckhoff who is the author of Cryptographic Militaire and Charles Briquet author of Les Filigranes. These books are mostly about Cryptography, but both contributed to the foundation of some Steganographic systems and more significantly to watermarking techniques.

d. Later stages following Steganographic techniques were adopted:

(i) Null Ciphers:- It is a Steganographic technique where the 3rd letter from each word in a harmless message is removed to create a hidden message.

(ii) Image substitution and microdot: In this Steganographic technique data such as pictures were reduced to the size of a large period on a piece of paper.

1.Digital Steganography

Digital Steganography is the process of embedding a secret data into the cover file and sending the cover file over the digital channel. Digital Steganographic techniques are classified as [5]

a. Early embedding: In early embedding the data is embedded before any other processing starts. This includes the spatial and transform domain techniques like DCT, DWT, LSB.

b. Delayed embedding: Delayed embedding is done after the video completes its processing. Methodologies include PVD (Pixel Value Differencing), bit streams etc.,

c. Intermediate embedding: The intermediate embedding is performed while the processing of the video is taking place. The techniques include intra and inter predictions, motion vectors, etc.

Let us discuss different techniques of digital steganography.

A] Early Embedding

Early embedding basically are done in two ways

1. Spatial domain

Spatial Domain is defined as a simple method where the secret information is embedded directly in the intensity of pixels. It means some pixel values of the image or video are changed directly to the pixels of the secret message while hiding the data [8]. Least significant bit (LSB) steganography is one of the easiest techniques that hides secret information in the LSBs of pixel values without any distortions. Changes in the value of the LSB are invisible to human eyes.

Spatial domain is used most often, where that is, over how many pixels does a cycle of periodically repeating intensity variations occur. It refers to the number of pixels over which a pattern repeats (its periodicity) in the spatial domain.

Spatial domain Techniques are classified into different categories:

a. Pixel Value Differencing(PVD) : The pixel-value differencing (PVD) scheme provides high imperceptibility to the Stego file. It is a technique where two consecutive pixels are selected and design a quantization range table to determine the payload by finding the difference value between the two selected consecutive pixels. Besides, it also offers the advantage of conveying a large number of payloads, while still maintaining theconsistency of an image characteristic after data embedding. The PVD highly depends on the difference between the two consecutive pixel values selected. In this method, first, we divide the cover image into non-overlapping blocks havingtwo connected pixels. At this point we adjust every block difference into the original pixel value. In a smooth area, the distinction between adjacent pixels is less than the edge range. Because of this more data is embedded into edge area pixels than in smooth areas. The Pixel Value Differencing (PVD) is better than Least Significant Bit (LSB) [9].

b. Most Significant Bit (MSB): In the MSB technique, the secret information is embedded into the most significant bit of the pixel in the image.

Example:

Cover file:

01001011 **0**1101010 **0**0011010
10111100 **0**1101010 **0**1001110
01111010 **1**0101011 **1**1011010

Secret message- 240 its binary equivalent is
011110000

Stego File:

01001011 **1**1101010 **1**0011010
10111100 **1**1101010 **0**1001110
01111010 **0**0101011 **0**1011010

c. Least Significant Bit:

The process of bit substitution means changing LSB bit of host media with bits of data (secret message). There are no visual differences (as seen with human eyes) between embedded and original media because the changes are very slight. This substitution technique works well for image, audio, and video steganography [10]

Example:

Cover file:

Framework of 3 pixels of a 24-bit image is represented as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

Secret Data: a message ―A‖ need to be hidden Character –A‖ is represented by the number 65, so that the equivalent 8-bit binary representation is
‗01000001'

Stego file:After embedding –A‖ (01000001) into LSB of cover file, we get a stego file as follows: (0010110**0** 0001110**1** 1101110**0**)
(1010011**0** 1100010**0** 0000110**0**)
(1101001**0** 1010110**0** 0110001**1**)

These changes due to hidden information are not visible to human eye and is capable of storing information from the first byte to the last.

d. Quantization Index Modulation (QIM):

A Quantization Index Modulation-based technique is a technique where information is embedded in the original sample values. Typical QIM is performed by modulating a signal with the embedded information after this, the Quantization process performed with the help of associated quantizer. QIM Achieves a good rate of performance by minimizing the distortion.

e. Random Pixel Embedding (RPE)

The ―random pixel embedding‖ (RPE) technique is a technique to embed the confidential data in facial area of the sub-band. In this technique the combination of alexnet and contourlet transform is used to generate good visual quality of the Stego image after embedding the confidential data.

f. Transform domain

Here are few Algorithms that does steganography using early embeddin g technique

DCT: Discrete Cosine Transform (DCT) is a well- known stegnographic technique in which text message is embedded in the least significant bits of the Discrete Cosine (DC) Coefficient of digital picture. In DCT technique, a RGB image is used as a secret image which is embedded in a compressed video (.mp4) having resolutions, frame rates and sizes. In DCT, we select the frames from the sequence of video frames with the help of appropriate Stego key, and then non-dynamic pixels of these frames are identified. The least significant bits (LSB) of the Discrete Cosine (DC) Coefficient of digital picture are used as carrier object for hiding the R, G, and B components of secret message individually.

DWT: Discrete Wavelet Transform (DWT) is a technique that transforms the frame from a spatial domain to a frequency domain where the wavelet coefficients are modified according to the secret message. DWT technique transforms the frame into four sub band frequency coefficients. These sub bands are as follows: low-low frequency (LL), horizontal band High - Low Frequency(HL), Vertical Band Low - High Frequency (LH) and Diagonal band High Frequency Tape. (HH). The LL sub band includes most of the important information of the spatial domain cover frame, and the other bands contain high-frequency data, such as edge information. Embedding data message into the frame in DWT domain is done as follows 1. The secret data that has to be hidden is converted to binary form. Then the cover video is divided into different frames. Algorithm will select a frame randomly from the video using key. Then the data will be embedded into the cover frames using asecret key.

FFT: A fast Fourier transform (FFT) algorithm computes the discrete Fourier transform (DFT) of asequence of data, or its inverse (IDFT). Fourier analysis converts a signal from its original domain such as time or space to a representation in the frequency domain and vice versa. The DFT divides a sequence of values into components of different frequencies. A Fast Fourier Transformation computes transformations

by factorizing the Discrete Fourier Transform matrix into a product of sparse (mostly zero) factors. Due to this method it manages to reduce the complexity of computing the DFT from O(N2) to O(NlogN), where N is the data size Many FFT algorithms are been designed based on a wide range of published theories, starting from simple complex-number arithmetic to group theory and number theory.

B] Intermediate Embedding

It includes following techniques

Intra predictions: The latest video coding standard H.265 and high efficiency video coding (HEVC), published by the Video Coding Experts Group (VCEG) of ITU-T and the ISO/IEC Moving Picture Experts Group (MPEG), has high compression performance, increased video resolution and abundant application scenarios. To improve the visual quality of carrier video, The algorithm analyze the embedding error of data hiding with modifying partitioning parameters of CB (coding blocks), PB (Partitioning block) and TB (Transform block), and it modifies the transform block decision to embed secret message and update corresponding residuals synchronously. In order to minimize the error during the embedding of the secret message, we utilize an efficient embedding mapping rule that can embed N (N>1) bits message and at most modify one bit transform partitioning flag in the cover video[13]

Inter predictions: In Inter prediction technique the embedding of the secret message is done by mapping seven block sizes of H.264 inter frame prediction such as 16x16, 16x8, 8x16, 8x8, 8x4, 4x8 and 4x4 to a number of bits from the secret message. The data hiding capacity of inter frame prediction is limited. Mapping rules of different block sizes can be used to embed the secret data in this technique.[14]

Motion vectors: In video compression, motion vector is the key element in the motion estimation process. of the cover video It is used to represent a macro block in a frame based on the position of this macro block in another frame. Motion vector qualities, for example, horizontal and vertical components, amplitude, and phase angles are used in embedding secret information. This method embeds information to pixels of frames in host video which is based on the H.264/AVC Video coding standard. It is designed a motion vector component feature to control embedding, and also to be the secret carrier. The information embedded will not significantly affect the video sequence‘s visual invisibility and statistical invisibility [14]

C] Delayed Embedding

It includes following technologies

PVD: Pixel Value Differencing(PVD) technique efficiently identifies the edge and smooth regions from an image, therefore, the PVDS technique is more suitable for concealing the secret information in an image In PVD algorithm grey-level images are used as the cover image and variable-sized secret message bit sequences are embedded into the cover image. Very few bit sequences from the secret message are embedded into the smooth region compared with the edge region. Initially, the cover image is divided into non-overlapping blocks of size 1×2 in raster scan order. Two consecutive pixels in the i^{th} block are labeled as Pi and Pi+1, respectively. The difference value, di, is calculated between two consecutive pixels using $d_i = |P_i - P_{i+1}|$. The absolute value of di denotes the differences present in each block. A small value of di means the presence of a smooth region, whereas a larger value indicates the presence of the edge region.

Bit streams: In order to avoid the leakage of video content , data hiding can be done directly in a video bit stream. H.264 is an industry standard for video compression, In this process the digital video is converted into a specific format that will take up less capacity when it is stored or transmitted. Video compression (or video coding) is an essential technology in the area such as digital television, DVD-Video, mobile TV, videoconferencing and internet video streaming. Standardizing video compression is useful for products from different manufacturers (e.g. encoders, decoders and storage media) to inter-operate. There is an encoder which will converts video into a compressed format and a decoder will do the reverse process of converting compressed video back into an uncompressed format. An Efficient data hiding approach on encrypted compressed video bit streams for privacy information protection based on, H.264/AVC coder and Bits replacement method H.264/AVC/MPEG-4 Part 10 allows it to compress video much more efficiently than older standards and to provide more flexibility

for application to a wide variety of network environments. Reduced time consumption process, It is useful to perceive video tampering Better compatible system for people privacy protection [15].

IV.COMPARATIVE ANALYSIS OF STEGANOGRAPHY ALGORITHMS

Above table 1 shows the comparison of various steganography algorithm discussed in this paper. The comparison is done on parameters such as payload, robustness, Performance,

Technique	Domain	Advantages	Other Parameaters
Pixel Value Differencing	Spatial	PVD provides, high embedding capacity of hidden datain the coverfile, withoutmuch noticeable distortion in cover file.	Better PSNR >45
Most SignificantBit	Spatial	Provides with better capacity and security	PSNR >41
Least SignificantBit	Spatial	Supports high capacityfor data hiding and high invisibility and robustness	PSNR = 56% DB
Quantization Index Modulation	Spatial	Better performance	PSNR >45
Random Pixel Embedding	Spatial	Gives good payload. Image retrieval by unauthorized user is difficult.	PSNR >40
Discrete Cosine Transform	Transform	DCT Provides high payload By embedding large volumeof data with minimal tradeoffs andhigh robustness [17].	Mean Square Error (MSE) B/w the two cases that there are no notable change s[18]
Discrete Wavelet Transform	Transform	This technique provides better performance, since it has high embedding payload and robustness. [17]	PSNR> 35.5 EN b/w 0.2 to 0.19

security and PSNR value. All the algorithm have their own way of hiding secret data in the cover image. The above comparison parameter values depend on the technique of data hiding. It is being analyzed that almost all the algorithm have high payload, i.e., they can embed high volume of data in the cover image.

V. CONCLUSION

In this paper we have tried to analyze and compare all the steganographic algorithms that have been developed through all these years by different research scholars.

This paper presented a clear view of the term steganography. Steganography is not a new technique, it has its roots in history as we have discussed in the first part of this paper. Gradually steganography has changed its forms. Now is the age of the digital era. The main focus of steganography is to preserve confidential information from hackers over the communication channel.

Comparative analysis of various steganography algorithms shows us that every algorithm is different from others in terms of data hiding capacity, complexity, level of cover file distortion etc.

In the current era of digitization, there is always a need for improvement of the current steganography algorithms. So our future research work will be to develop efficient and accurate Steganography algorithms, either by combining the existing techniques or by developing new techniques.

REFERENCES

[1] Dr. Nitika Arora, ―Types and tools of Steganography‖ ,International Journal for Research, volume 10, jun 22
[2] https://www.simplilearn.com/what-is-steganography- article
[3] Kaur, Harpreet & Rani, Jyoti. (2016). A Survey on different techniques of steganography. MATEC Webof Conferences.5702003. 10.1051/matecconf/20165702003.
[4] Dragoş Dumitrescu and Ioan-Mihail Stan and Emil Simion, ―Steganography techniques‖, Cryptologyeprint Archive
[5] G R, Manjula and R B, Sushma, Video Steganography: A Survey of Techniques and Methodologies (May 22, 2021). Proceedings of the International Conference on Smart Data Intelligence (ICSMDI 2021).
[6] Al-khafaji, Ali & Nur, Nilam & Sjarif, N.N.A.. (2020). A Review of Comparative Spatial Domain Techniques of Steganography and Watermarking. Technology Reports of Kansai University. 62. 12.

[7] Dalal, M., Juneja, M. (2018). Video Steganography Techniques in Spatial Domain—A Survey. In: Mandal, J., Saha, G., Kandar, D., Maji, A. (eds) Proceedings of the International Conference onComputing and Communication Systems. Lecture Notes in Networks and Systems, vol 24. Springer, Singapore.

[8] Hsien-Wen Tseng, Hui-Shih Leng, "A" Rani, Mary & S. Lakshmanan, & G Deepalakshmi (2017). Study on video Steganography using spatial Domain.

[9] Patel, R., Lad, K., Patel, M. et al. An efficient DCT- SBPM based video steganography in compressed domain. Int. j. inf. tecnol. 13, 1073–1078 (2021).

[10] Rabie, Tamer. (2012). Digital Image Steganography: An FFT Approach. Communications in Computer and Information Science. 294. 10.1007/978-3-642-30567- 2_18.

[11] H. Zhao, Y. Liu, Y. Wang, S. Liu and C. Feng, "A Video Steganography Method Based on Transform Block Decision for H.265/HEVC," in IEEE Access, vol. 9, pp. 55506-55521, 2021, doi: 10.1109/ACCESS.2021.3059654.

[12] Angitha John, Anjana Baby, "A Survey on Video Steganography", International Journal of Science and Research (IJSR), Volume 8 Issue 4, April 2019, pp.800-805.

[13] Vengadalakshmi, S. Abiramasundari, "Secret Data Hiding in Compressed Video Bit Streams for Privacy Information Protection", International Journal of Science and Research (IJSR), Volume 4 Issue 4, pp.3075-3078, April 2015.

[14] A P, Sherly & Sapna, Sasidharan & Amritha, P.. (2010). A Compressed Video Steganography using Random Embedding Scheme. International Journal of Computer Science and Information Security. 8.

[15] Mansi Dave, Hinal Somani, ―A SURVEY ON DIGITAL VIDEO STEGANOGRAPHY TECHNIQUES USED FOR SECURE TRANSMISSION OF DATA‖, JARIIE-ISSN(O)-MP4 VIDEO STEGANOGRAPHY USING LEAST SIGNIFICANT BIT (LSB) SUBSTITUTION AND ADVANCED ENCRYPTION STANDARD (AES) 1 PUTU ARI SRI LESTARI EKA NINGSIH, 2 GUSTI MADE ARYA SASMITA, 3 NI MADE IKA MARINI MANDENNI


April 2024
Vol- 14 No.- 4
@ IJITCE Publication